IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN RE: DEALER MANAGEMENT SYSTEMS ANTITRUST LITIGATION	MDL No. 2817 Case No. 18-cv-00864
This Document Relates To: *Authenticom, Inc. v. CDK Global, LLC, et al.*, Case No. 1:18-cv-00868 (N.D. Ill.)	Hon. Robert M. Dow, Jr. Magistrate Judge Jeffrey T. Gilbert **PUBLIC-REDACTED**

PLAINTIFF AUTHENTICOM, INC.'S OPPOSITION TO COUNTERCLAIMANT REYNOLDS AND REYNOLDS COMPANY'S MOTION FOR PARTIAL SUMMARY JUDGMENT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITY

GLOSSARY

Abbreviation	Full Citation
ACOM SUF	Authenticom, Inc.'s Statement of Undisputed Material Facts in Support of Its Motion for Summary Judgment on Defendants' Counterclaims (Dkt. 977)
Antitrust Opp.	Authenticom, Inc.'s Opposition to Defendants CDK Global, LLC's and The Reynolds and Reynolds Company's Motion for Summary Judgment
CC Br.	Authenticom, Inc.'s Memorandum of Law in Support of Its Motion for Summary Judgment on Defendants' Counterclaims (Dkt. 978)
PJ RSUF	MDL Plaintiffs' Joint Response to Defendants CDK Global, LLC and The Reynolds and Reynolds Company's Joint Statement of Common Undisputed Material Facts in Support of Their Motions for Summary Judgment
PJ SAF	MDL Plaintiffs' Statement of Additional Facts in Opposition to Defendants' Motion for Summary Judgment (filed concurrently)
Dorris Ex.	Exhibits to the Declaration of Daniel V. Dorris in Support of Plaintiff Authenticom, Inc.'s Motion for Summary Judgment on Defendants' Counterclaims (Dkt. 977-1)
Emmanual Ex.	Exhibits to the Declaration of Jonathan Emmanual in Support of The Reynolds and Reynolds Company's Motion for Partial Summary Judgment (Dkt. 779-2)
Ho Ex.	Exhibits to the Declaration of Derek T. Ho in Support of MDL Plaintiffs' Oppositions to Defendants' Motions for Summary Judgment
Wilkinson Ex.	Exhibits to the Declaration of Brice Wilkinson in Support of Reynolds's Motion for Partial Summary Judgment (Dkt. 779-1)

INTRODUCTION

Defendants The Reynolds and Reynolds Company ("Reynolds") and CDK Global, LLC ("CDK") have brought civil counterclaims under federal and state criminal statutes – the Digital Millennium Copyright Act ("DMCA") and the Wisconsin Computer Crimes Act ("WCCA") – to deflect scrutiny from their own antitrust violations. For the reasons Authenticom, Inc. ("Authenticom") has given in its summary judgment motion, those counterclaims fail as a matter of law. But, as explained below, they at best raise factual questions for trial. Reynolds's summary judgment motion – which CDK has not joined – should be denied.

I. A jury could reasonably find that Authenticom did not violate the DMCA because (1) Reynolds's dealer contracts expressly authorize dealers' agents to [redacted] the DMS, and (2) Authenticom was dealers' agent because dealers had the capability to control Authenticom's work.

II. Evidence of Defendants' anticompetitive conduct supports Authenticom's defenses under copyright misuse, fair use, and illegality doctrines. Because the DMCA imposes liability only where there is a nexus between circumvention of a technological measure and a copyright violation, Authenticom's copyright misuse and fair use defenses create factual disputes for trial. Similarly, the illegality doctrine bars Reynolds from invoking the DMCA to further its anticompetitive conduct.

III. Reynolds's DMCA claim implicates numerous factual disputes as to which instances of access (if any) violated the DMCA.

A. The statute of limitations bars Reynolds from asserting DMCA liability for any instances of access prior to June 29, 2015. Reynolds asserts several methods of access violated the DMCA – including so-called "memory ripping" and "Menu Walks" – without any proof that those methods were used during the limitations period and in the face of evidence that a jury could reasonably determine shows those methods of access ended much earlier.

B. A jury could reasonably conclude that Authenticom did not "circumvent" Reynolds's CAPTCHA or Suspicious User ID Monitoring ("ID Monitoring") program because Authenticom obtained access to Reynolds's DMS only by using valid dealer-supplied login credentials and by accurately responding to CAPTCHA prompts. Reynolds's assertion that Authenticom made "efforts" to obtain access by other means is flawed; there is no DMCA liability for "attempted" circumvention.

C. The DMCA applies only where the technological measures "control[ ] access to a [copyrighted] work." 17 U.S.C. § 1201(a)(1)(A). Reynolds asserts the copyrighted works are its "software code" and executables. A jury could reasonably conclude that no technological measure prevented access to Reynolds's code or executables; indeed, Reynolds offers no contrary proof.

D. The essential characteristic of a technological measure covered by the DMCA is an ability to preclude access by those who lack authority. A reasonable jury could conclude that Reynolds's CAPTCHA and ID Monitoring fail that definition: CAPTCHA presented all the information needed to respond, and thus had no capability to preclude access; ID Monitoring did not require prospective users to do anything to gain access.

IV. Unlike the DMCA, the WCCA prohibits only "willful" and "knowing" unauthorized access. Authenticom employees have unanimously testified that they believed their access of Reynolds's DMS was properly authorized by dealers – a belief backed by the industry's pervasive use of data integrators for more than a decade – including with Reynolds's awareness and consent. A jury could easily credit that testimony and reject Reynolds's WCCA claim.

BACKGROUND

Most of the material facts are set forth in Authenticom's summary judgment motion on Reynolds's counterclaims (CC Br.) and in Authenticom's concurrently filed opposition to

Defendants' motion for summary judgment on its antitrust claims (Antitrust Opp.). To avoid repetition, Authenticom incorporates those facts here and additionally states as follows:

I. Reynolds's dealer contracts provide that the dealer and its [redacted] *See* CC Br. 16. Dealers consider Authenticom their agent for providing data integration services, and dealers may control all aspects of Authenticom's data integration service. They can direct which data to provide to which app vendors, and the timing and frequency of delivery. Dealers can monitor which data Authenticom delivers to which app vendors and when. Dealers can also direct Authenticom to stop providing data integration services at any time. Authenticom has accessed Reynolds's DMS only with express, written authorization from dealers. *See id.* at 10-12.

Historically, Authenticom provided data integration services to Reynolds dealers via "user emulation," as did other data integrators such as DMI and IntegraLink. *See id.* at 10-11, 13-14. At various times, Reynolds has tried to frustrate data integrators' access via user emulation, including through (1) CAPTCHA prompts that display a distorted image of text that the user must answer before proceeding, and (2) ID Monitoring that disables certain login credentials. *See id.* at 19-22. Authenticom maintained its ability to access Reynolds's DMS in three relevant ways.

Whitelisting. Reynolds agreed to allow Authenticom to continue providing data integration services for certain dealers. *See id.* at 16; ACOM SUF 69-70; PJ SAF 27-28. For these dealers, Reynolds's CAPTCHA and ID Monitoring measures appear to have often (but not always) been disabled. *See* Wilkinson Ex. 33 [Dkt. 779-35], at -204 ("These [whitelisted] logons *typically* do not have Captcha.") (emphasis added).

CAPTCHA. Authenticom responded to the CAPTCHA by entering the text that was displayed on the screen; it never bypassed a CAPTCHA without entering the correct response. *See*

CC Br. 20. Authenticom responded to CAPTCHA in four ways: (1) it had employees and temporary workers review and respond to the CAPTCHA manually; (2) it used software to interpret the CAPTCHA on the screen; (3) it sent an image of the CAPTCHA to a vendor (DeathByCaptcha) whose workers provided Authenticom the answer; and (4) for a brief period that ended by June 2014 (outside the limitations period), Authenticom used a program called "Auto CAPTCHA" to "read" the CAPTCHA answer from computer memory. *See* ACOM SUF 91-98.

ID Monitoring. In May 2013, Reynolds started disabling login credentials that Reynolds claimed were "suspicious." ACOM RSUF 17. Over the following months, Authenticom's DMS accounts were periodically disabled, followed by periods of few (if any) accounts being disabled. *See* PJ SAF 91. Reynolds issued guidance to its dealers that one "solution" to disabled credentials was to "set up a temporary user ID for the third party," though noting this was a "stop-gap approach" that might "violate the Dealers' Customer Agreement with Reynolds." ACOM SUF 86; Dorris Ex. 144 [Dkt. 977-146], at -094.[1] Authenticom tried several changes to its access methods so that Reynolds's ID Monitoring program would not disable its login credentials, but the only method that was successful was for a dealer to provide a new login credential to Authenticom. *See* CC Br. 21; ACOM SUF 85.

Over time, dealers became less willing to continue providing Authenticom with new login credentials, causing Authenticom to either lose the dealer's business or the dealer to switch to a dealer-driven push method. *See, e.g.*, Emmanual Ex. 93 [Dkt. 783-2], at -727. While Reynolds allows Authenticom to use this dealer-driven push method, *see* ACOM RSUF 6-8, it is not an adequate substitute for automated data integration. *See* PJ SAF 30. Authenticom must rely on

[1] *See also* Emmanual Ex. 30 [Dkt. 779-32], at -978 (directing dealers to review credentials flagged as "suspicious" and, "if the system administrator determines that the user needs to access the ERA® System, he should issue the user a new User ID set up with the correct access").

technologically savvy dealer employees to use the report generator tools in Reynolds's DMS (Dynamic Reporting) to export data and to send ("push") that data to Authenticom. *See id*. According to CDK and Reynolds, this method is "complex," "time consuming," and "inherently unreliable," and thus, is "not a viable alternative for data integration, period." *Id.* Since early 2016, Authenticom has been forced by Reynolds's blocking efforts to provide the vast majority of its data integration services to Reynolds dealers using Dynamic Reporting. *See* PJ RSUF 39.

LEGAL STANDARD

Authenticom incorporates the legal standard in its Antitrust Opposition brief.

ARGUMENT

I. THE JURY COULD REASONABLY DETERMINE THAT AUTHENTICOM HAD AUTHORIZATION TO ACCESS REYNOLDS'S DMS

Authenticom is entitled to summary judgment on Reynolds's DMCA claims on the basis that Authenticom acted as dealers' agent. *See* CC Br. 24-34, 38. At a minimum, it is entitled to trial on that issue.

If Authenticom was acting as dealers' agent when it accessed Reynolds's DMS, Authenticom did not violate the DMCA. Reynolds's dealer contracts provide that dealers and their [redacted]. Dorris Ex. 19 [Dkt. 977-20], Master Agreement § 1; Dorris Ex. 21 [Dkt. 977-22], Defined Terms. This Court has previously held – for a substantively identical provision in CDK's dealer contracts[2] – that "the phrase 'agents and employees' is not ambiguous"; the only question is "whether Authenticom falls within the scope of that language." *In re DMS Antitrust Litig.*, 362 F. Supp. 3d 558, 566 n.2 (N.D. Ill. 2019);

[2] Authenticom did not move to dismiss Reynolds's DMCA claim because Reynolds had yet to produce the "Defined Terms," which unambiguously establish that dealers' agents may access the DMS.

see also Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1204 (Fed. Cir. 2004) ("authoriz[ation]" provides "immun[ity]").

As this Court further noted, the question whether Authenticom acted as dealers' agent is an issue of fact, which "'seldom can be resolved at the summary judgment stage, much less on a motion to dismiss.'" *DMS*, 362 F. Supp. 3d at 569 (quoting *Restoration Specialists, LLC v. Hartford Fire Ins. Co.*, 2009 WL 3147481, at *3 (N.D. Ill. Sept. 29, 2009)). "Given that the existence of an agency relationship is a question of fact, rather than of law," summary judgment must be denied if there is "any conflicting evidence of an agency relationship." *Brainard v. Am. Skandia Life Assur. Corp.*, 432 F.3d 655, 661 (6th Cir. 2005) (governing Ohio law); *see NASCAR Holdings, Inc. v. Testa*, 97 N.E.3d 414, 417 (Ohio 2017). Here, there is abundant evidence of an agency relationship. *See* CC Br. 31-34; ACOM SUF 23-26, 32-44.

Reynolds's arguments to the contrary (at best) raise questions of disputed fact.

First, for reasons given in Authenticom's summary judgment motion, Reynolds is wrong (at 17 & n.57) that its contracts do not let dealers grant their agents access. The contract's language [redacted] – is unambiguous. *Second*, although Reynolds argues (at 17-18) that it did not "approve[]" of Authenticom's access, Reynolds's views cannot override the legal authorization conferred by the plain terms of the contract. *See* CC Br. 34-37. At the very least, a jury could reasonably determine that Authenticom's access was authorized notwithstanding Reynolds's preference to end that access, in light of the contrary provision in Reynolds's binding contracts with dealers.

Third, Reynolds's claims (at 18) that Authenticom needed "specific authorization" to respond to Reynolds's technological measures – not just authorization to access Reynolds's DMS – is incorrect under the DMCA because there must be a nexus to a copyright violation (which does

not exist if access is authorized). *See* CC Br. 38, 55-58. And a jury could reasonably conclude that dealers – in exercising their contractual right to have their agents "Use" the DMS – authorized Authenticom to respond to technological measures that improperly frustrated that "Use." Indeed, dealers repeatedly complained that Reynolds's CAPTCHA and ID Monitoring was impeding their right to use data integrators. *See* PJ SAF 33; Ho Ex. 109, at -156 [redacted]; Ho Ex. 441.[3]

II. A JURY COULD REASONABLY FIND AGAINST DMCA LIABILITY BASED ON COPYRIGHT FAIR USE AND ILLEGALITY

A. A Jury Could Reasonably Determine There Is No DMCA Liability Because There Is No Underlying Copyright Violation

The Fourth and Federal Circuits and three district courts in this circuit have correctly held that the DMCA requires a nexus between circumvention of a technological measure and a copyright violation. *See* CC Br. 55-58. Authenticom has two defenses to copyright liability that must be resolved by the factfinder.

1. As a threshold matter, summary judgment must be denied because Reynolds has failed to address, let alone negate, Authenticom's fair use defense. *See* Dkt. 517, at 65. A motion for summary judgment that "ignore[s] . . . affirmative defenses" is "facially defective"; the movant cannot address those defenses for the first time in its reply brief. *RB & W Mfg. LLC ex rel. RB & W Corp. v. Burford*, 2004 WL 2496242, at *4 (N.D. Ill. Nov. 4, 2004) (failure to negate affirmative defenses in a summary judgment brief requires denial of summary judgment); *see Becker v. Tenenbaum-Hill Assocs.*, 914 F.2d 107, 110, 112 (7th Cir. 1990).

[3] Reynolds's authority concerns different circumstances where the entity providing authorization specifically prohibited the use or access at issue. *See Synopsys, Inc. v. AzurEngine Techs., Inc.*, 401 F. Supp. 3d 1068, 1071 (S.D. Cal. 2019) (use of counterfeit license keys instead of permissible valid license keys); *Disney Enters., Inc. v. VidAngel, Inc.*, 869 F.3d 848, 863 (9th Cir. 2017) (unauthorized decryption of DVD instead of permissible use through DVD players).

Nor could Reynolds have adduced evidence to overcome Authenticom's fair use defense. Authenticom showed in its motion for summary judgment that it has a fair use defense as a matter of law. *See* CC Br. 58-60. At a minimum, a factfinder could reasonably find that Authenticom's access was fair use under the four factors in 17 U.S.C. § 107 and *Assessment Technologies of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640 (7th Cir. 2003). "[M]arket effect" (Paragraph 4) is the "most important" factor, *Kienitz v. Sconnie Nation LLC*, 766 F.3d 756, 758 (7th Cir. 2014), and favors Authenticom because Authenticom's use of Reynolds's DMS software will have no effect on the market for that software – dealers would still need to purchase DMS to operate their businesses. *See WIREdata*, 350 F.3d at 645; *Evolution, Inc. v. SunTrust Bank*, 342 F. Supp. 2d 943, 956 (D. Kan. 2004) (extracting data from database "will have no effect on the potential market" for the database). Further, the "nature of the copyrighted work" (Paragraph 2) here is "utilitarian" rather than "creative." *Denison v. Larkin*, 64 F. Supp. 3d 1127, 1134 (N.D. Ill. 2014); *Sega Enters. Ltd v. Accolade, Inc.*, 977 F.2d 1510, 1524 (9th Cir. 1992) ("[C]omputer programs are, in essence, utilitarian articles – articles that accomplish tasks."). The "amount" of copying was minimal (Paragraph 3) because Authenticom used Reynolds's DMS software only as an intermediate step in obtaining access to data stored on the DMS over which Reynolds can assert no copyright. *See* Antitrust Opp. 3-4; *WIREdata*, 350 F.3d at 644-45 (citing *Sega Enters.*, 977 F.2d at 1520-28).[4] Finally, Paragraph 1 "really only comes up when the alleged infringement substitutes for the copyrighted work in the market," which is not the case here as Authenticom is not a DMS provider. *Red Label Music Publ'g, Inc. v. Chila Prods.*, 388 F. Supp. 3d 975, 985 (N.D. Ill. 2019).

[4] *See also Ticketmaster Corp. v. Tickets.Com, Inc.*, 2003 WL 21406289, at *4 (C.D. Cal. Mar. 7, 2003) (fair use despite "momentary" copying while "non-protected material . . . is extracted"); *Nautical Sols. Mktg., Inc. v. Boats.com*, 2004 WL 783121, at *2 (M.D. Fla. Apr. 1, 2004) (same); *Evolution*, 342 F. Supp. 2d at 956 (fair use "to access and extract uncopyrightable data that was embedded in a copyrighted computer program").

2. Authenticom will also proffer evidence at trial that dealers "own" (that is, have a right to control) most, if not all, of the data stored in their DMS. *See* Antitrust Opp. 3-4. Reynolds seeks to leverage (jointly with CDK) its copyrighted database software (the DMS) to control that data, even though Reynolds has no ownership interest in that data. *See* Dorris Ex. 151 [Dkt. 977-153], Israel Rep. ¶¶ 12-13, 90, 100, 110, 118, 137, 205 (antitrust theory). A factfinder could reasonably find that this constitutes copyright misuse – that is, "leveraging" of a copyright owner's "limited monopoly to allow them control of areas outside the monopoly." *WIREdata*, 350 F.3d at 647 (internal quotation marks omitted); *see also qad. inc. v. ALN Assocs., Inc.*, 770 F. Supp. 1261, 1267 (N.D. Ill. 1991), *aff'd*, 974 F.2d 834 (7th Cir. 1992) ("egregious" copyright misuse in using copyright to "restrain . . . use of material over which [the plaintiff] itself had no rights").[5]

B. A Jury Could Reasonably Find That Reynolds's Unlawful Conduct Precludes Liability Under The DMCA

Reynolds cannot pursue claims for DMCA violations for the independent reason that the pursuit of those claims would further its unlawful conspiracy. The Supreme Court has recognized an "illegality defense" arising under the antitrust laws where a plaintiff's claims – if countenanced – would "enforce conduct that the antitrust laws forbid." *Kaiser Steel Corp. v. Mullins*, 455 U.S. 72, 81-82 (1982). In *Kaiser*, a union sued to enforce payments to health and retirement funds due under a collective bargaining agreement that required coal producers to make extra payments to the funds if they purchased coal from other producers not under contract with the union. *See id.* at 74-76. The Supreme Court held that, if – as alleged by the plaintiff coal producer – the collective bargaining provision requiring these extra payments violated the antitrust laws, the plaintiff would

[5] The doctrine of misuse covers a broader range of conduct – and is easier to establish – than the antitrust violations at issue in this MDL. *See Nielsen Co. (US), LLC v. Truck Ads, LLC*, 2011 WL 221838, at *6 (N.D. Ill. Jan. 24, 2011).

have a defense to any suit seeking to enforce those payments. *See id.* at 85-86; *see also Robbins v. Lynch*, 836 F.2d 330, 333-34 (7th Cir. 1988) (applying illegality defense).

Applying the illegality defense to statutory causes of action like the DMCA is necessary to avoid an implied repeal of the Sherman Act. *See Kaiser Steel*, 455 U.S. at 88. Prior to the enactment of the DMCA, well-established principles of antitrust law (and copyright misuse) would have forbidden Reynolds from colluding with its competitor CDK to eliminate data integrators (a group boycott) and would have made illegal Reynolds's blocking efforts to enforce that agreement. *See* Antitrust Opp. 40-41. The DMCA did not impliedly repeal that preexisting law. *See Chamberlain*, 381 F.3d at 1201-02 ("The DMCA, as part of the Copyright Act, does not limit the scope of the antitrust laws, either explicitly or implicitly. . . . 'Repeal of the antitrust laws by implication is not favored and not casually to be allowed.' ") (quoting *Gordon v. N.Y. Stock Exch., Inc.*, 422 U.S. 659, 682 (1975)).[6]

Authenticom's antitrust claim implicates this illegality defense. The technological measures at issue were how Reynolds enforced its conspiracy with CDK to block data integrators. *See* Antitrust Opp. 22-29. Imposing liability for DMCA violations would thus "enforce conduct that the antitrust laws forbid." *Kaiser Steel*, 455 U.S. at 81-82; *see Chamberlain*, 381 F.3d at 1201

[6] Even the Ninth Circuit – the only circuit to reject the "nexus" requirement for the DMCA – has recognized that "attempting to enforce [a] DMCA anti-circumvention right in a manner that violates antitrust law" would require analysis of the "interplay" between the DMCA and antitrust law. *MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 951 (9th Cir. 2010); *see also Broadcast Music, Inc. v. Columbia Broad. Sys., Inc.*, 441 U.S. 1, 19 (1979) (observing that "the copyright laws confer no rights on copyright owners . . . to violate the antitrust laws"); *United States v. Microsoft Corp.*, 253 F.3d 34, 63 (D.C. Cir. 2001) ("[Microsoft] claims an absolute and unfettered right to use its intellectual property as it wishes: '[I]f intellectual property rights have been lawfully acquired,' it says, then 'their subsequent exercise cannot give rise to antitrust liability.' . . . That is no more correct than the proposition that use of one's personal property, such as a baseball bat, cannot give rise to tort liability.") (citation omitted); *Data Gen. Corp. v. Grumman Sys. Support Corp.*, 36 F.3d 1147, 1187 (1st Cir. 1994) ("[T]he Copyright Act does not explicitly purport to limit the scope of the Sherman Act. . . . [W]e must harmonize the two [Acts] as best we can."); *In re Indep. Serv. Antitrust Litig.*, 203 F.3d 1322, 1325 (Fed. Cir. 2000) ("Intellectual property rights do not confer a privilege to violate the antitrust laws.").

(refusing to interpret the DMCA to allow a manufacturer to "wrap the copyrighted material in a trivial 'encryption' scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing products" in violation of antitrust law). It is no answer that Reynolds, as a technical matter, could have imposed these measures apart from the conspiracy with CDK. *See Kaiser Steel*, 455 U.S. at 79 (rejecting argument that contract provision "standing alone" was not illegal where the entire "undertaking is illegal"). Nor does it matter that *some* of Reynolds's technological measures were imposed prior to September 2013. That merely raises a factual dispute whether, after September 2013, Reynolds would have been able to maintain and extend its blocking measures given the competitive pressures that Reynolds would have faced absent the conspiracy. *See* Antitrust Opp. 8-15.

III. ADDITIONAL FACTUAL DISPUTES PRECLUDE SUMMARY JUDGMENT ON REYNOLDS'S DMCA CLAIM

Notwithstanding Reynolds's request (at 26) for summary judgment as to all Authenticom's varied methods of access over a multi-year period, the law requires Reynolds to prove that each instance of access satisfies the DMCA's elements. *See* 17 U.S.C. § 1203(c)(3)(A) (providing statutory damages "per act of circumvention"). Summary judgment should be denied because there are factual disputes regarding which instances of access (if any) give rise to DMCA liability.

A. There Are Factual Disputes Regarding Which Instances Of Access Fall Outside The Statute Of Limitations

Reynolds may not pursue DMCA claims based on instances of access before June 29, 2015. *See* Dkt. 225 (counterclaims filed June 29, 2018); 17 U.S.C. § 507(b) (three-year statute of limitations); CC Br. 60-62. Even if Reynolds's DMCA claims related back to Authenticom's complaint (they do not), instances of access prior to May 1, 2014 would be time-barred. *See* CC Br. 63-65. As set forth below, Reynolds has failed to meet its burden of establishing that many of the methods of access it challenges were in use after June 29, 2015 (or May 1, 2014).

Auto CAPTCHA. Authenticom has presented evidence that Auto CAPTCHA was not used past May 1, 2014, and Reynolds presents none to the contrary. *See* ACOM SUF 98; Dorris Ex. 165 [Dkt. 977-167], Clements Decl. ¶ 11. In the evidence relied on by Reynolds, the most recent reference to Auto CAPTCHA was in a February 26, 2014 email, but that email indicates Authenticom had stopped using Auto CAPTCHA. *See* Wilkinson Ex. 46 [Dkt. 780-5], at -097. Authenticom's Software Manager for DMS Integration advocated switching to "a single way to manage the CAPTCHA answering" and "assum[ed]" that would be the "ManualCAPTCHA process" where "an actual person enter[s] input." *See id.*

Database of CAPTCHA answers. Reynolds claims (at 11) that Authenticom responded to ASCII CAPTCHA – CAPTCHA that is displayed as text characters on a screen – by a human manually determining the response to specific prompts, storing that response in a database, and having Authenticom's software provide that same response if the same prompt was encountered subsequently. *See* Wilkinson Ex. 40 [Dkt. 779-42], Brown Tr. 170:20-71:21. But – as Reynolds acknowledges (at 10) – Reynolds phased out ASCII CAPTCHA in 2012. *See* ACOM SUF 81-83.

Menu Walk. Reynolds asserts (at 14) that Authenticom's software "walk[ed]" through menus in Reynolds's DMS software so that the ID Monitoring program did not flag Authenticom's accounts. But Reynolds's documents show that, as of July 3, 2013, Authenticom "disabl[ed] all menu walks" by removing "the application that runs them" so "they will not actually execute." Wilkinson Ex. 74 [Dkt. 782-25], at -433 (Email from H. Dearman (July 3, 2013)); Wilkinson Ex. 71 [Dkt. 782-22], at -310 (Email attachment sent on May 13, 2015: "****PLEASE NOTE** – per 7/3/13 email from Heidi, no longer using Menu Walk*"). Reynolds claims that Menu Walk was used into 2016 based on a chat transcript from May 18, 2015 in which an Authenticom employee suggests "we'll have to menu walk" but not before "test[ing] the theory," Wilkinson Ex. 75 [Dkt.

782-26], at -801, and a February 2016 list of 350 locked profiles for which a single dealer is listed as "Norman Frede Chevrolet Menu Walk," Wilkinson Ex. 76 [Dkt. 782-27], at -493. At best those two documents are conflicting evidence; they do not support summary judgment.[7]

B. A Jury Could Reasonably Determine That Authenticom Did Not Circumvent Any Technological Measures

There are disputed factual issues regarding which (if any) of Authenticom's methods of responding to Reynolds's CAPTCHA and ID Monitoring were "circumvention" under the DMCA. The DMCA prohibits only descrambling, decrypting, avoiding, bypassing, removing, deactivating, or impairing a technological measure. *See* 17 U.S.C. § 1201(a)(3)(A). Reynolds asserts (at 12-19) only that Authenticom engaged in "bypassing" or "avoiding." Authenticom has shown that, as a matter of law, it did not "bypass" or "avoid" the CAPTCHA or ID Monitoring because Authenticom always provided the information required by those measures. *See* CC Br. 41-46. Even if Reynolds has a viable claim, it raises factual disputes.

CAPTCHA – Reynolds's CAPTCHA required that Authenticom respond to prompts like the following that stated, "human interaction is required." *See* Dorris Ex. 155 [Dkt. 977-157], Miracle Rep. ¶ 79.

[7] Reynolds's characterization of the sole purpose of Menu Walk being to "fool" Reynolds is inaccurate. Menu Walk was used to maintain a persistent connection to the DMS so that Authenticom's software did not need to repeatedly log in and out. *See* ACOM RSUF 41.

Several of the challenged methods of responding to this CAPTCHA *did* involve "human interaction." For example, DeathByCAPTCHA, [redacted] where humans would interpret and respond to the CAPTCHA. ACOM SUF ¶¶ 94-95. Reynolds also asserts (at 11) that it was unlawful for Authenticom to have its own employees and temporary workers respond to CAPTCHA, but a jury could reasonably conclude that Authenticom responded to the CAPTCHA prompts by the very means required by the prompts – "human interaction" – and that Authenticom did not "bypass" or "avoid" the prompts. Indeed, CDK (unlike Reynolds) does not seek to hold Authenticom liable for humans responding to CAPTCHA. *See* Dorris Ex. 148 [Dkt. 977-150], Stroz Rep. App'x C, ¶¶ 2, 4-17; Dorris Ex. 147 [Dkt. 977-149], Rubinfeld CDK Rep. ¶¶ 58-61.

ID Monitoring – Reynolds claims (at 14-16) that Authenticom made "efforts" to circumvent the ID Monitoring program. But the DMCA does not prohibit *attempted* circumvention, *see* CC Br. 44-46, and Reynolds does not offer any evidence (or even assert) that Authenticom *actually* circumvented the program such that its login credentials would no longer be disabled. Indeed, Reynolds never specifically explains how the monitoring process worked, much less how Authenticom could (or ever did) avoid or bypass any aspect of the process that was disabling its credentials. *See, e.g.*, ACOM RSUF 47-48; Wilkinson Exs. 68, 79 [Dkts. 782-19, 782-30] (continued disabling of credentials despite Authenticom's "efforts"); *see also* Wilkinson Ex. 76 [Dkt. 782-27] (February 2016: requesting dealers create new credentials for 350 disabled profiles); Wilkinson Ex. 19 [Dkt. 779-21], at -940 (two solutions: "regularly schedule the generation of a new user profile" or dealer-driven push). Reynolds's damages expert likewise does not even attempt to determine the number of times Authenticom supposedly circumvented

the ID Monitoring program. *See* Dorris Ex. 152 [Dkt. 977-154], Rubinfeld Reynolds Rep. ¶ 74 n.88.[8]

There is evidence that the only means available to Authenticom to maintain its data integration service on Reynolds's DMS after its existing login credential had been disabled by Reynolds's ID Monitoring was to request new login credentials from the dealer. *See* ACOM SUF 85. CDK, which encountered the same blocking, reached the same conclusion. *See* Dorris Ex. 125 [Dkt. 977-127]. And a jury could reasonably conclude that the only effective method – requesting new login credentials – was not circumvention. After its credentials were disabled, Authenticom received messages directing Authenticom to "contact your System Administrator" – that is, the *dealer* employee responsible for provisioning login credentials. *See, e.g.*, Wilkinson Ex. 32 [Dkt. 779-34], at -453. Further, Reynolds advised dealers that, when faced with this situation, they could create a new "temporary user ID for" the affected party. *See supra* p. 4 & n.1. A jury could reasonably conclude that, by following the process that Reynolds created for obtaining replacement login credentials, Authenticom did not avoid or bypass ID Monitoring.

C. Reynolds Has Failed To Satisfy Its Burden Of Establishing That Its Technological Measures Protected Any Copyrighted Work

There are disputed issues of fact regarding whether any of Reynolds's technological measures "control[led] access" to a copyrighted work. 17 U.S.C. § 1201(a)(1)(A); *see Lexmark Int'l Inc. v. Static Control Components, Inc.*, 387 F.3d 521, 550 (6th Cir. 2004) ("To the extent the [work] is not a 'work protected under [the copyright statute],' . . . the DMCA necessarily would not protect it."). Reynolds asserts (at 7-8, 20) that the "copyrighted work" is the executable code

[8] Reynolds's overstated rhetoric about Authenticom's efforts is unwarranted. As but one example, Reynolds states "Authenticom even resorted to deleting records and reports off the DMS to hide its tracks," but the documents that Reynolds cites show only a concern that leaving data reports on the DMS might take up too much space. *See* ACOM RSUF 44; *see generally* Dorris Ex. 154 [Dkt. 977-156], Shostack Rep. ¶ 163 (considering and rejecting claim that Authenticom acted like a "hacker").

of its DMS software. *See* Wilkinson Exs. 9-12 [Dkts. 779-11–14] (copyrights).[9] As Authenticom has explained, none of Reynolds's technological measures controlled access to executable code, which could be executed without encountering a CAPTCHA prompt or supplying login credentials (which were disabled by ID Monitoring). *See* CC Br. 46-47. A jury could reasonably conclude based on this evidence that neither CAPTCHA nor the ID Monitoring program prevented access to Reynolds's executable code, thus requiring denial of Reynolds's motion for summary judgment.

In its counterclaims, Reynolds alleged that the copyrighted work also included the visual elements of Reynolds's DMS software that are displayed after the software has been executed – the "screen layouts, graphical content, and text." Dkt. 225, Reynolds Counterclaims ¶¶ 30-31, 119. But allegations are insufficient at summary judgment. Reynolds needed to proffer competent evidence that the visual elements protected by Reynolds's technological measures and accessed by Authenticom were protected by copyright. *See Lexmark Int'l*, 387 F.3d at 550. But Reynolds's motion makes no showing – by expert evidence or otherwise – as to which visual elements were protected by Reynolds's technological measures, which visual elements were accessed by Authenticom, and whether any of those visual elements exhibited sufficient creativity to be subject to copyright protection. *See Apple Computer, Inc. v. Microsoft Corp.*, 35 F.3d 1435, 1443-44 (9th Cir. 1994) (noting that not all visual elements of software are protected by copyright). There is also record evidence that the technological measures at issue – in particular CAPTCHA – did not appear until after Authenticom had already accessed almost every visual element of Reynolds's DMS and that the few remaining visual elements were not copyrightable. *See* CC Br. 48-49. Reynolds's motion for summary judgment cannot be granted on this record.

[9] Reynolds incorrectly states (at 20) that Authenticom created a copy of Reynolds's software on its server for each instance of access. *See* ACOM RSUF 26.

D. A Jury Could Reasonably Determine That Reynolds's Technological Measures Did Not Effectively Control Access

The DMCA applies only to "technological measure[s]" that "*effectively* control access," which means that the measure must "in the ordinary course of its operation, require[ ] the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3)(B) (emphasis added). This provision requires that the "technological measure" be capable of distinguishing between those who have "authority" from the copyright owner and those who do not. *See* CC Br. 49-51. Authenticom has shown that summary judgment must be granted in its favor because neither Reynolds's CAPTCHA nor its ID Monitoring had that capability. *See id.* at 51-54. At a minimum, factual disputes prevent summary judgment in Reynolds's favor, because the jury must determine whether the capabilities of Reynolds's technological measures qualify them for DMCA protection.

Among other things, both sides' experts have analyzed the technological measures at issue and have reached different conclusions regarding the nature and capabilities of those measures, and ultimately, whether those measures qualify as security access controls as understood by computer security experts. Authenticom's expert Nancy Miracle has opined that none of Reynolds's technological measures had any capability to determine whether the user attempting to access the DMS was appropriately authorized, and, as such, would not be considered security access controls. *See* Dorris Ex. 155 [Dkt. 977-157], Miracle Rep. ¶¶ 31-34, 41-43, 78-80, 113-16. Reynolds's security expert Scott Tenaglia disagreed. *See* Tenaglia Reply Rep. 20-23. This is "a classic battle of the experts" that the jury will need to resolve. *Gicla v. United States*, 572 F.3d 407, 414 (7th Cir. 2009).

IV. SUMMARY JUDGMENT CANNOT BE GRANTED ON REYNOLDS'S WCCA CLAIM BECAUSE THERE ARE DISPUTED FACTS REGARDING AUTHENTICOM'S AUTHORIZATION AND INTENT

Summary judgment cannot be granted on Reynolds's WCCA claim because there are disputed facts regarding Authenticom's authorization, *see supra* Part I, and because Reynolds's anticompetitive conduct gives rise to an illegality defense, *see supra* Part II.B. There also is sufficient evidence from which a jury could reasonably conclude that Authenticom did not "willfully, knowingly and without authorization" "[a]ccess[ ] computer programs" or "[d]isclose[ ] restricted access codes" in violation of the WCCA. Wis. Stat. 943.70(2)(a)(3) & (6). Reynolds cannot meet the "willfully" and "knowingly" requirements if Authenticom had a subjective belief that its acts were authorized. *See Wisconsin v. Scheurell*, 1995 WL 131927, at *1 (Wis. Ct. App. Mar. 29, 1995); *Boyd v. Wisconsin*, 258 N.W. 330, 335-36 (Wis. 1935) (interpreting "willfully" to mean "knowingly commit[ing] an act prohibited by a criminal statute") (quoting *Hobbins v. Wisconsin*, 253 N.W. 570, 574 (Wis. 1934)).

Authenticom employees testified that they did not understand accessing Reynolds's DMS using dealer-provided credentials to be "unauthorized" because they believed they were properly authorized as dealers' agent (not a third party). *See* ACOM SUF 28. These "denial[s] of knowledge" present a dispute of material fact that must be resolved by the jury unless they are "so utterly implausible in light of conceded or irrefutable evidence that no rational person could believe [them]." *In re Chavin*, 150 F.3d 726, 727-28 (7th Cir. 1998); *see Primex Plastics Corp. v. Zamec*, 2016 WL 750669, at *2 (W.D. Wis. Feb. 24, 2016) ("If the party denies that it acted with the required intent and the party's testimony is not incredible as a matter of law, then the issue must be resolved by the factfinder rather than as a matter of law."); *Day v. City of Baraboo*, 2007 WL 5633174, at *6 (W.D. Wis. Jan. 31, 2007) ("Once the defendant testifies that he did not have [an

unlawful] motive . . . it would be the rarest of instances in which the plaintiff could prevail at summary judgment. A court would have to conclude that the defendant was lying . . . .").

Authenticom's employees' testimony easily satisfies that plausibility standard. Their beliefs were backed by the years-long practice of dealers and app vendors pervasively relying on data integrators to access data on every type of DMS. *See* CC Br. 9-15. CDK was the largest provider of data integration services (at least prior to its conspiracy with Reynolds) and used the same methods of access as Authenticom; [redacted] *See id.* at 14-15; *see also* ACOM SUF 71 (same for another data integrator). And Reynolds – despite its current bombastic rhetoric – used Authenticom's data integration service for years, even on Reynolds's own DMS. *See* CC Br. 10. Further, dealers represented that their use of Authenticom's data integration service would not breach their DMS contracts. *See* Dorris Ex. 104 [Dkt. 977-106], §§ 7.1 ("Each Party represents and warrants that . . . its entrance into these Terms and Conditions does not violate any agreement between such Party and any third party."), 10.15 ("Each Party further represents that it has not entered into, nor will it enter into, any agreements that would conflict with its obligations under these Terms and Conditions or would render it incapable of satisfactory performing hereunder."). Authenticom was entitled to rely on these representations. *See Hocking v. City of Dodgeville*, 785 N.W.2d 398, 405 (Wis. 2010) ("[A] warranty is generally defined as an assurance by one party to a contract of the existence of a fact upon which the other party may rely. . . . A warranty is intended to relieve the promisee of any duty to ascertain the fact for himself.").

Reynolds's desire to end Authenticom's access and its preference that all app vendors use Reynolds's RCI data integration service would not prevent a reasonable jury from crediting Authenticom employees' testimony that they subjectively believed that the company's access was

authorized by the relevant party – the dealers that own the data. Nor would the threatening letter that Reynolds sent to Authenticom in April 2015. That letter claimed that its contracts with dealers barred dealers from "allow[ing] access . . . by third parties," Emmanual Ex. 91 [Dkt. 782-42], but Authenticom was dealers' agent, not a third party, *see* CC Br. 31-34. Moreover, when Authenticom tried to confirm these contractual provisions, Reynolds sent heavily redacted "form" agreements that had been filed in other litigation and that omitted the provisions that gave authorization to dealers' agents. *See* Wilkinson Ex. 90 [Dkt. 782-41], at -038, -048. Other publicly filed documents in that litigation showed there was a dispute whether Reynolds's dealer contracts allowed the use of data integrators. *See* Second Decl. of Jeanne Crandall ¶¶ 7-8, *The Reynolds & Reynolds Co. v. Superior Integrated Sols., Inc.*, No. 12-848 (S.D. Ohio Nov. 25, 2013), Dkt. 69-1 (averring that Reynolds had produced DMS contracts "contain[ing] specific provisions allowing for third party integration"). A reasonable jury could find that Authenticom – caught between a dispute between dealers (which thought they could use data integrators to access Reynolds's DMS, as they had for years) and Reynolds (which claimed they could not) – had a good-faith subjective belief that the dealers' authorization was sufficient, consistent with the terms of their contracts and longstanding industry practice.[10]

CONCLUSION

Reynolds's motion for summary judgment should be denied.

[10] Reynolds's sole authority is distinguishable. In *Epic Systems Corp. v. Tata Consultancy Service Ltd.*, 2016 WL 4033276 (W.D. Wis. July 27, 2016), there was no dispute that the defendant consultant would have been allowed to access plaintiff's database software for "integration" (which is what Authenticom did). *Id.* at *2. But the consultant accessed the plaintiff's technical documentation for other purposes (allegedly to develop a competing product), *see id.* at *7, *10-11, and there was no dispute that such access had not been authorized, *see id.* at *23.

Dated: July 28, 2020

Respectfully submitted,

/s/ Derek T. Ho

Derek T. Ho
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com

Counsel for Plaintiff Authenticom, Inc.

CERTIFICATE OF SERVICE

I, Derek T. Ho, an attorney, hereby certify that on July 28, 2020 I caused a true and correct copy of the foregoing **PLAINTIFF AUTHENTICOM, INC.'S OPPOSITION TO COUNTERCLAIMANT THE REYNOLDS AND REYNOLDS COMPANY'S MOTION FOR PARTIAL SUMMARY JUDGMENT** to be filed and served electronically via the court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the court's CM/ECF system. Copies of the Under Seal filing were served on counsel of record via email.

/s/ Derek T. Ho

Derek T. Ho
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com